Homeland Security and Defense Center

A MULTI-UNIT RESEARCH CENTER

Adversary Adaptation to Protective Measures

Brian A. Jackson

Senior Physical Scientist

MORS Working Group 1 –
Optimizing Domestic Security Response to Adaptive Adversaries

November 16, 2010

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
16 NOV 2010		**00-00-2010 to 00-00-2010**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Adversary Adaptation to Protective Measures	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Rand Corporation,Homeland Security and Defense Center,PO Box 2138,Santa Monca,CA,90407-2138**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
Optimizing Investments in Critical Infrastructure Protection, 15?18 Nov 2010; ANSER Conference Center, Arlington, VA. U.S. Government or Federal Rights License

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**25**	

To Plan Well We Need To "Reasonably Anticipate" Adversary Adaptation and Its Potential Effects

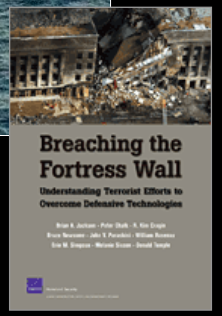
- ***"The goal of this session is to think intelligently & systematically about how adversaries adapt to our investments in infrastructure protection, and how we can plan security accordingly."***
- **Thinking intelligently about adaptation requires:**
  - **Characterizing the range of options available to adversaries**
  - **Understanding the factors that shape the choices that they make and their ability to change effectively**
- **Linking that understanding to security planning requires:**
  - **Analyzing the effect of different types of adaptation on security effectiveness**
  - **Understanding how "adaptation externalities" groups face affect the risk they pose more broadly**
- **Both these topics have implications for what data is needed for assessing the overall effectiveness (effects?) of security efforts**

Briefing Outline

- *"The goal of this session is to think intelligently & systematically about how adversaries adapt to our investments in infrastructure protection, and how we can plan security accordingly."*
- **What we know about adversary adaptation to security measures**
  - **Characterizing the range of options available to adversaries**
  - **Understanding the factors that shape the choices that they make and their ability to change effectively**
- **Building a comprehensive picture of adaptation *effects* on risk**
  - **Analyzing the effect of different types of adaptation on security effectiveness**
  - **Understanding how "adaptation externalities" groups face affect the risk they pose more broadly**
- **Concluding observations on analysis and data collection needs**

What Do We Know About Adversary Adaptation In Response To Security Investments?

- **Adversaries – terrorist, criminal, and other groups – often change their behavior in response to security measures**
  - **Not all adaptation that affects security performance is *caused* by the security measures themselves**
  - **But many of the more troubling ones are – particularly from the perspective of security planners**



Photos: Wikimedia Commons

Adversaries Have A Wide Variety of Adaptation Options Available To Them

Modifying their *operational designs* to avoid detection technologies and other countermeasures

RAND

Photos: Wikimedia Commons

Adversaries Have A Wide Variety of Adaptation Options Available To Them

Modifying the *weapons technologies* they use to circumvent defensive efforts

Constructing improvised mortar systems to:

- *throw larger shells over security perimeters*
- *allow timed or remote operation to escape preventive patrol operations*

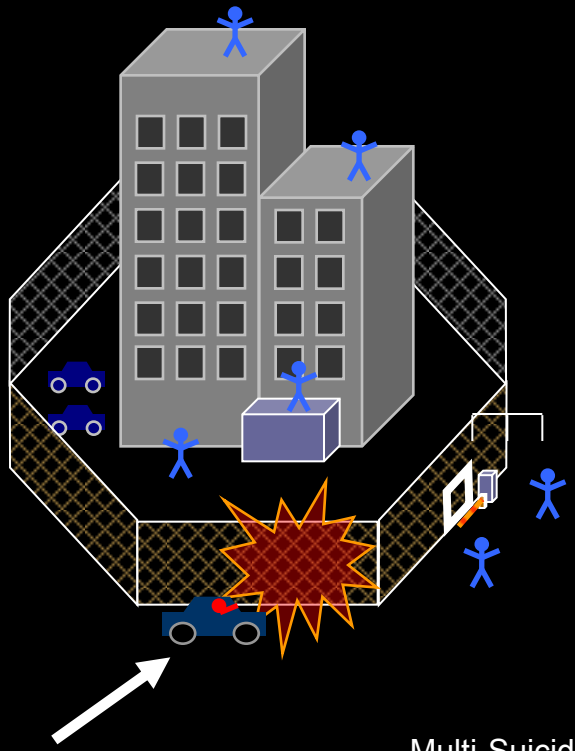
Photos: Wikimedia Commons, PIRA propaganda videos

Adversaries Have A Wide Variety of Adaptation Options Available To Them

Increasing the *complexity* of their operations to include direct attack on defensive measures

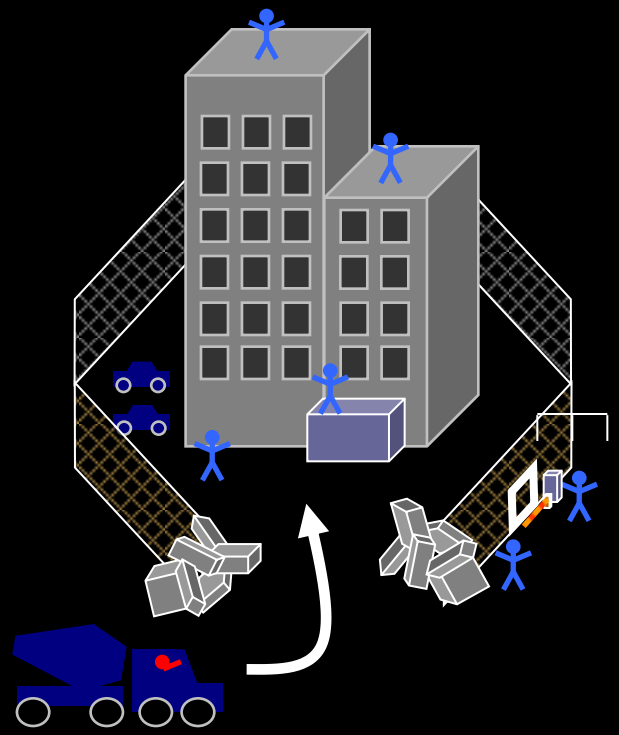
1

An initial suicide vehicle bomb strikes the perimeter wall around the target.



2

With the perimeter broken, a second enters through the breach to strike.



Multi-Suicide Vehicle Bomb Attack on Palestine Hotel
Baghdad, Iraq
October 24, 2005

Attack included a third vehicle that detonated prematurely

RAND

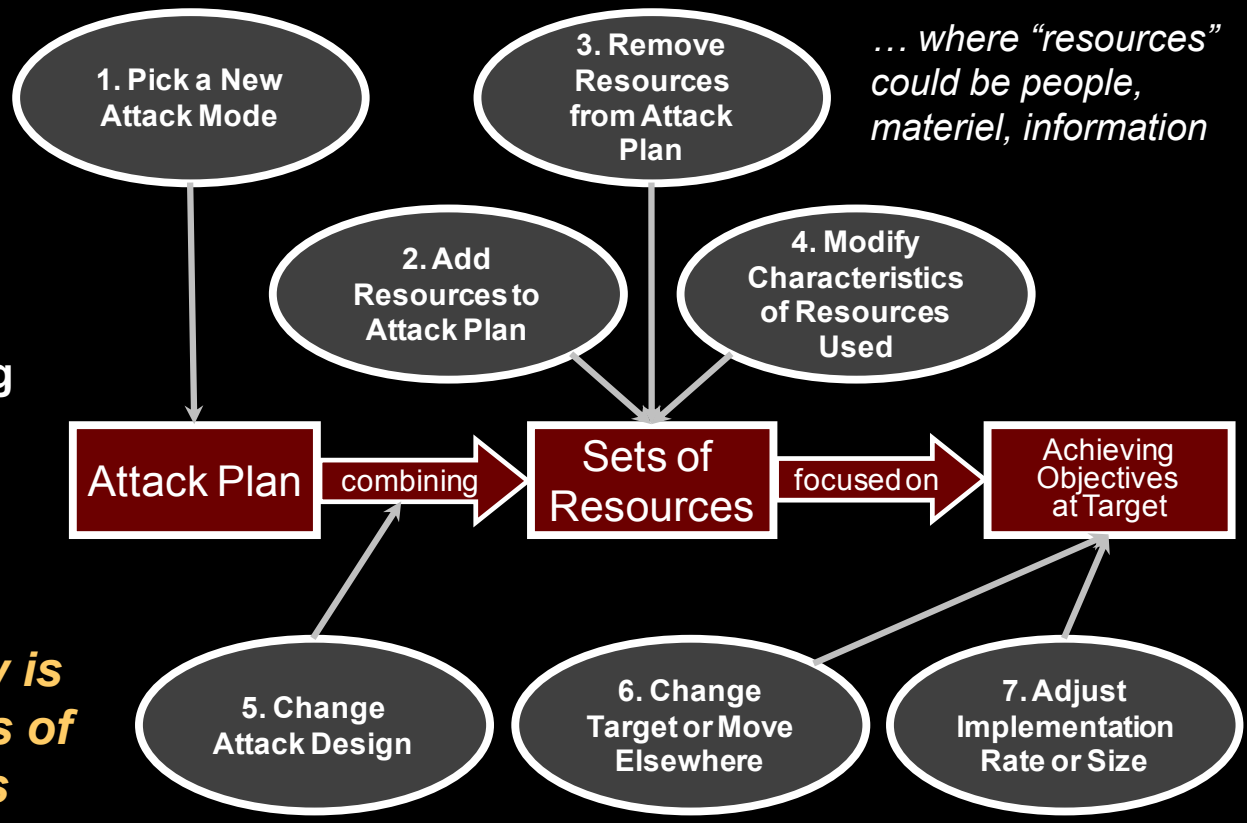
Description from *Washington Post*, Oct 25, 2005.

Moving From Anecdotes To a Taxonomy Of Attacker Adaptation Options

In response to a defensive challenge, a group could:

- **Change itself**
  - **Reorganize**
  - **Adjust internal processes**
- **Change its activities**
  - **Alter what it is doing**
  - **How it is doing it**
  - **Where it is doing it**
  - **Etc.**

An ongoing RAND study is examining different ways of categorizing attackers adaptation paths



Note: Diagram focused on attack behavior, but could be generalized.

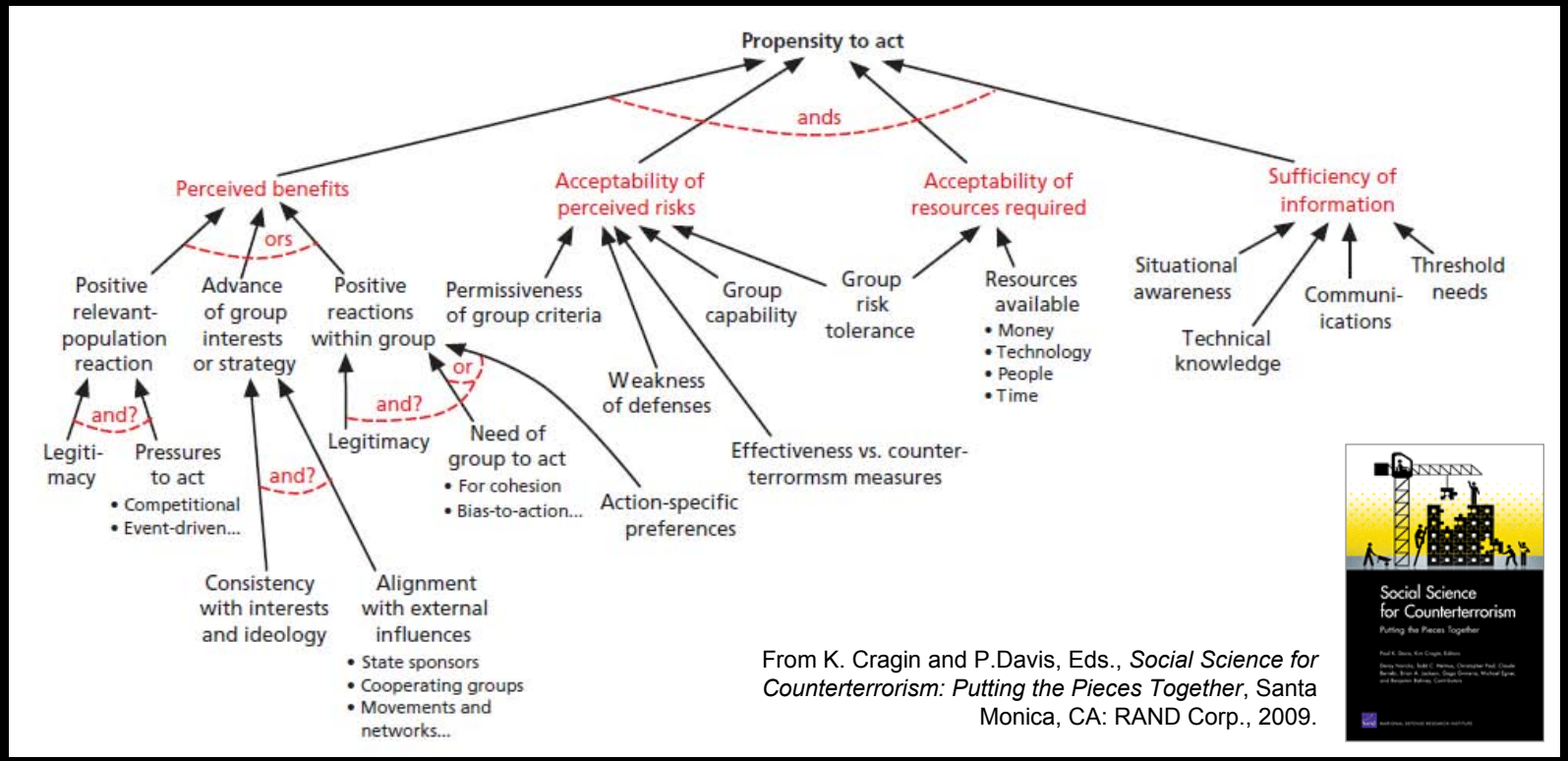
When Considering Their Behavior, We Cannot Forget Adversary Groups Are Human Organizations…

- **Though adversaries' full set of adaptation options is a useful starting point…**
  - **… It is unrealistic to assume they will choose and implement the "optimal" path out of that option set**
- **As human organizations, adversaries must deal with:**
  - **Imperfect information**
  - **Organizational idiosyncrasies and preferences**
  - **Human dysfunctions in decision making**
  - **Limits on the ability to successfully implement their chosen course of action**
- **As a result, a specific adversary may not even consider all options, may base its choice among them on "wrong" information, and may not be able to pull off what it decides to do**

Anticipating adversary behavior requires understanding how they actually act, not how they ideally might behave

Anticipating How A Specific Group Will Adapt Requires Digging Into Its Decision Process…

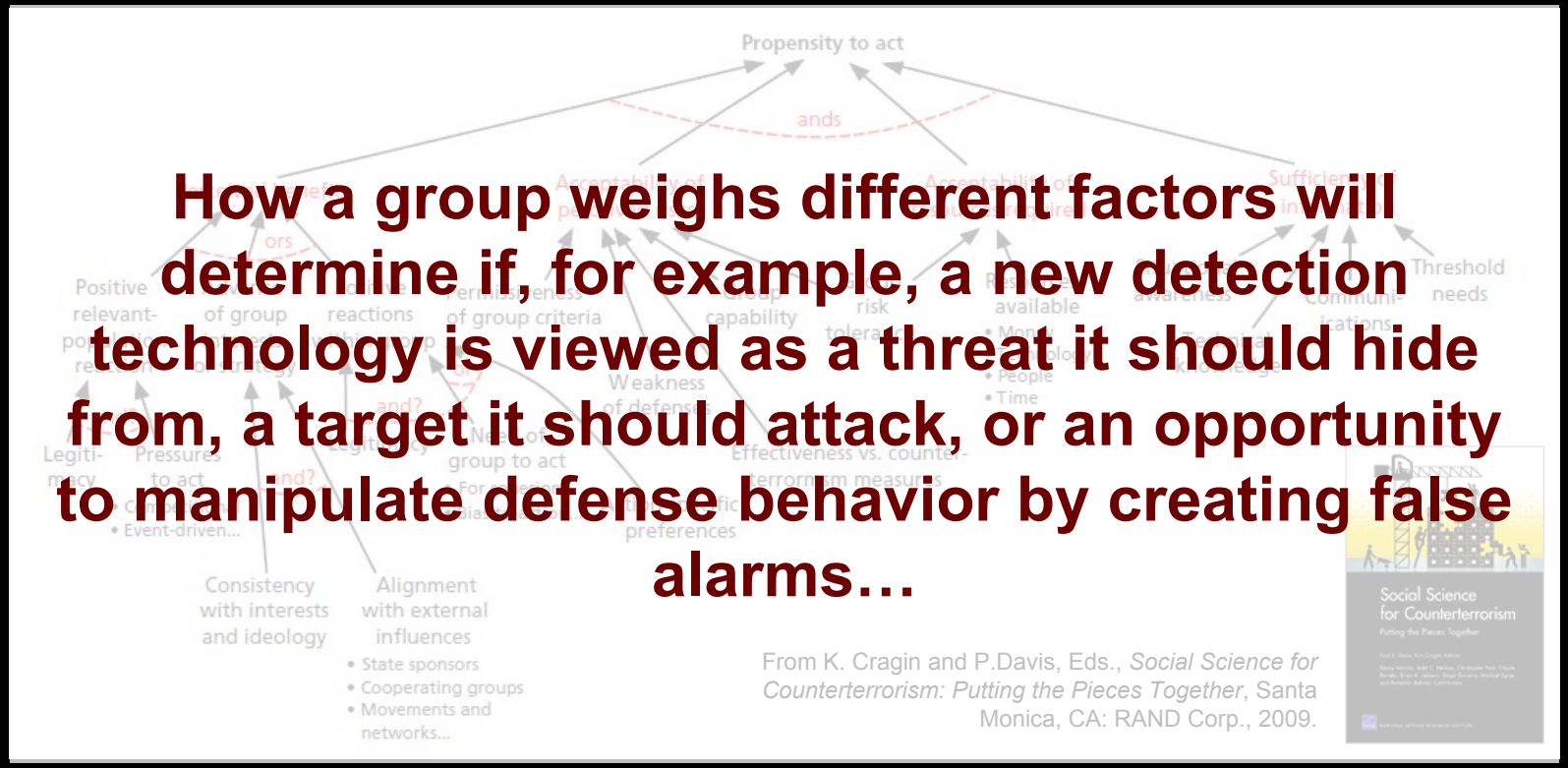
- **Group's choices are shaped by internal and external factors**
- **Choices are generally a sort of cost-risk-benefit comparison, though may be a very imperfect one**
  - **Different adaptation options have different costs, risks, etc.**



From K. Cragin and P.Davis, Eds., *Social Science for Counterterrorism: Putting the Pieces Together*, Santa Monica, CA: RAND Corp., 2009.

Anticipating How A Specific Group Will Adapt Requires Digging Into Its Decision Process…

- **Group's choices are shaped by internal and external factors**
- **Choices are generally a sort of cost-risk-benefit comparison, though may be a very imperfect one**
  - **Different adaptation options have different costs, risks, etc.**



How a group weighs different factors will determine if, for example, a new detection technology is viewed as a threat it should hide from, a target it should attack, or an opportunity to manipulate defense behavior by creating false alarms…

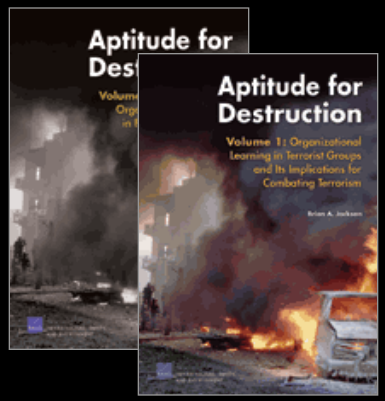
From K. Cragin and P.Davis, Eds., *Social Science for Counterterrorism: Putting the Pieces Together*, Santa Monica, CA: RAND Corp., 2009.

…And Anticipating Whether Or Not It Will Succeed Requires Understanding Its Capabilities

- A group without the ability to adapt may gain nothing from attempting to do so
  - New more damaging explosive device… that doesn't go off.
- Social science has identified a variety of factors that affect groups' capability to adapt
- Even if it is successful in responding to a defensive measure, is the change "local" or "global:"
  - Just the innovator knows?
  - Part of the group can do it?
  - The entire group has the capability?

Factors shaping innovative & adaptive capability include:

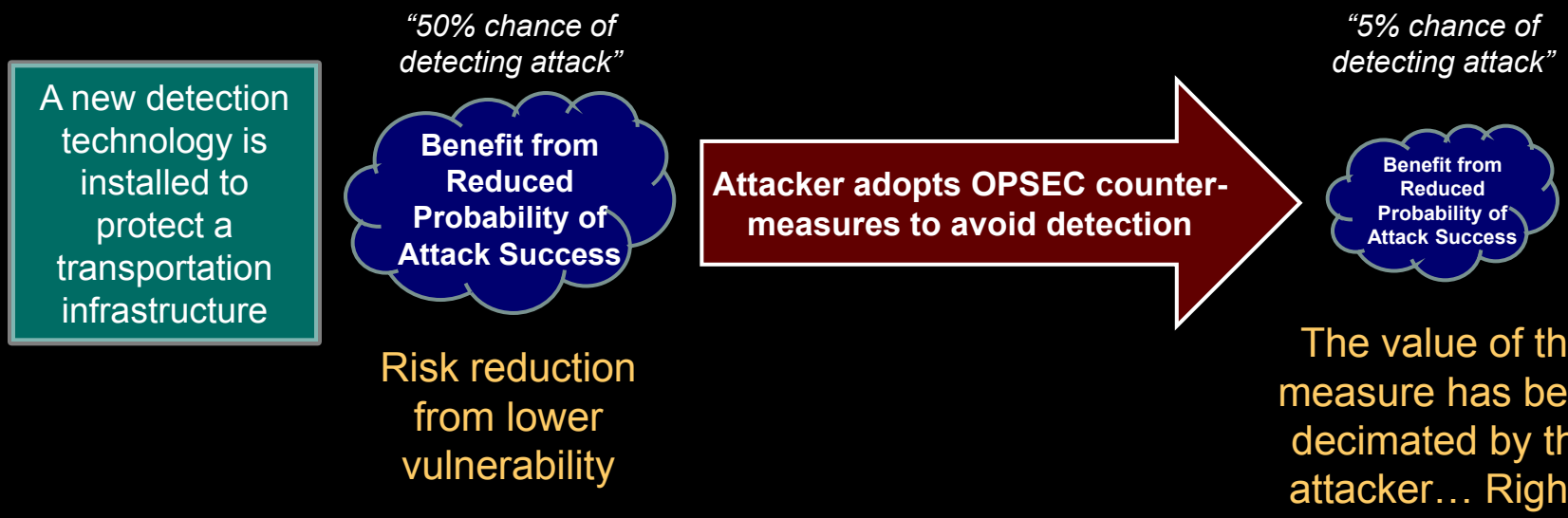
- Leadership and structure
- Group culture
- Communications modes (internal and external)
- Absorptive capacity for new knowledge or technology
- Group environment
- Stability of membership
- Resources available
- Attitude toward risk



Briefing Outline

- **What we know about adversary adaptation to security measures**
  - **Characterizing the range of options available to adversaries**
  - **Understanding the factors that shape the choices that they make and their ability to change effectively**
- **Building a comprehensive picture of adaptation *effects* on risk**
  - **Analyzing the effect of different types of adaptation on security effectiveness**
  - **Understanding how "adaptation externalities" groups face affect the risk they pose more broadly**
- **Concluding observations on analysis and data collection needs**

We Often Think About Adaptation Effects On Security From A Very Local Perspective

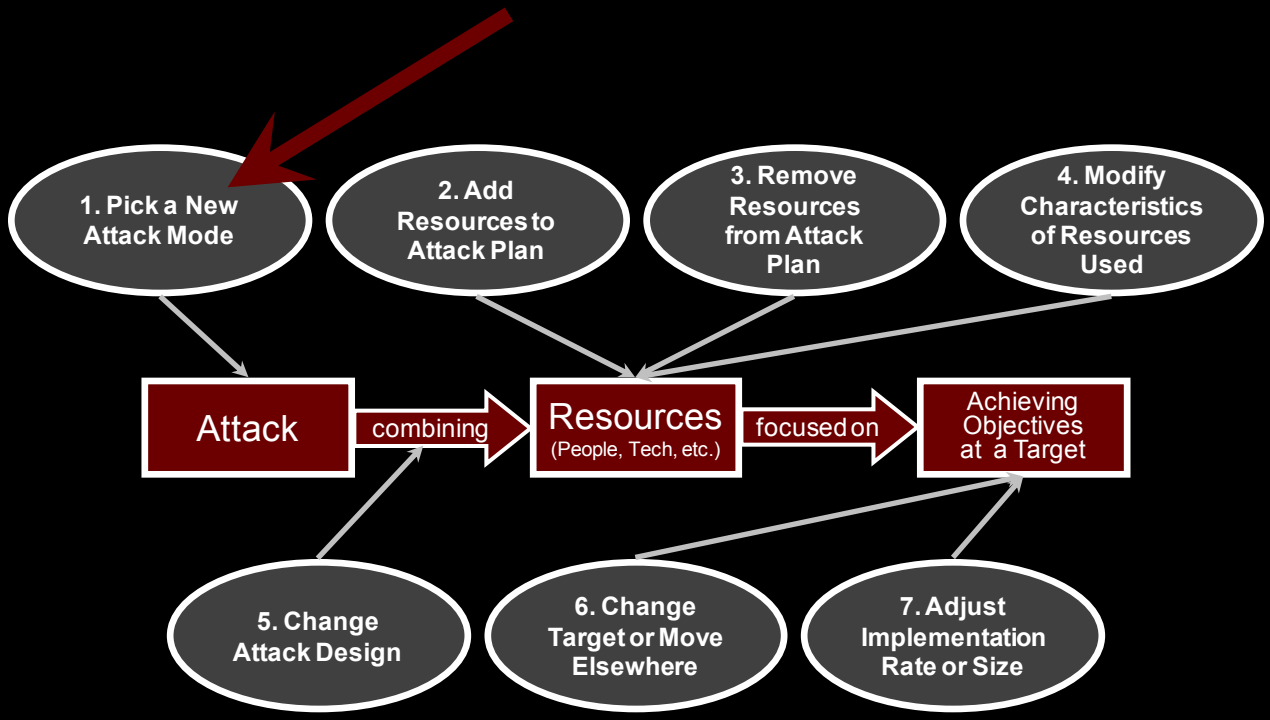


- **Tendency is to think about effects of adaptation in a binary way**
  - "Adaptation X makes security measure Y ineffective"
- **An adaptation's effect on security functionality *does not necessarily* equal its effect on risk… even at the target protected by the measure**
  - In the example above, what if the OPSEC effort tripled the resources required to stage an attack?
  - Adaptation means vulnerability is only cut 1/10 what was expected, but (holding attack resources constant) threat is cut by 2/3… so the defense is still ahead.

Different Adaptation Paths Have Varied Effects On Risk… And Value Depends On Perspective

If attackers pick a new attack mode in response to protections at a target, risk could go up or down:

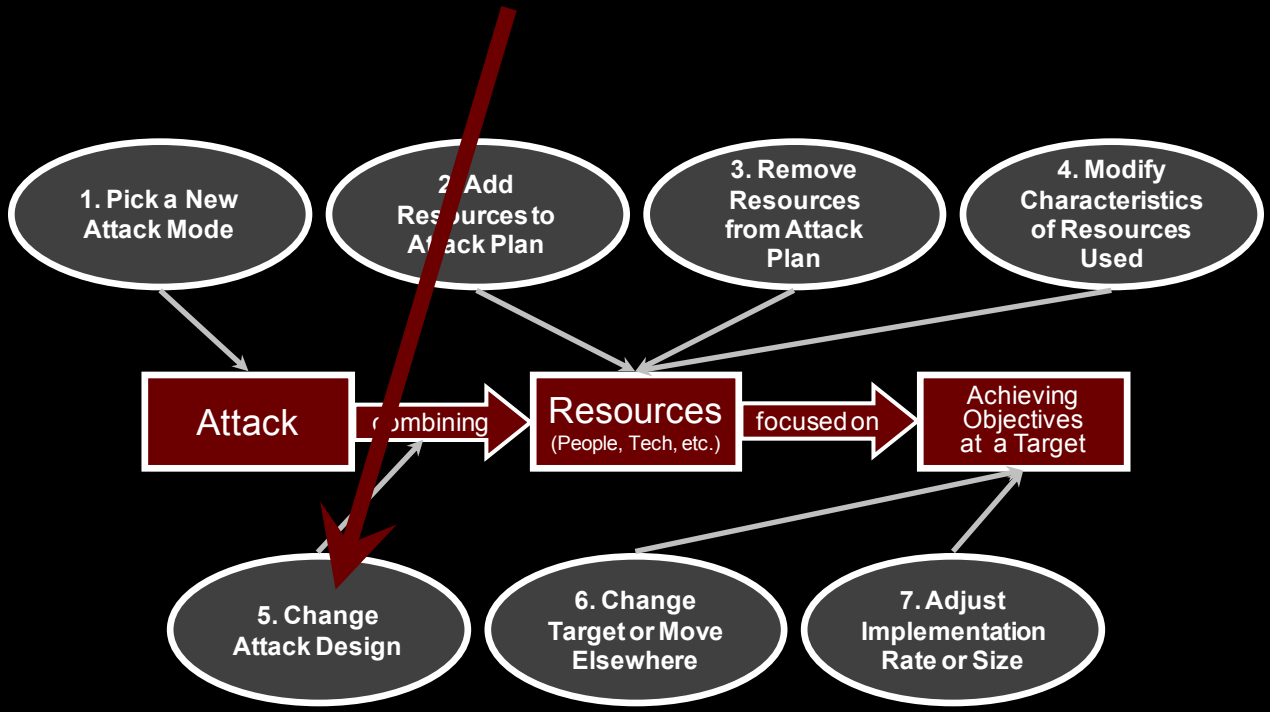
- **More damaging mode → ΔRisk + at protected target**
- **Less damaging mode → ΔRisk – at protected target (though attack frequency might remain constant)**



Different Adaptation Paths Have Varied Effects On Risk… And Value Depends On Perspective

If attackers "answer" to a defensive investment is a more complex attack design, risk will decrease… though the link to the security measure may not be obvious:

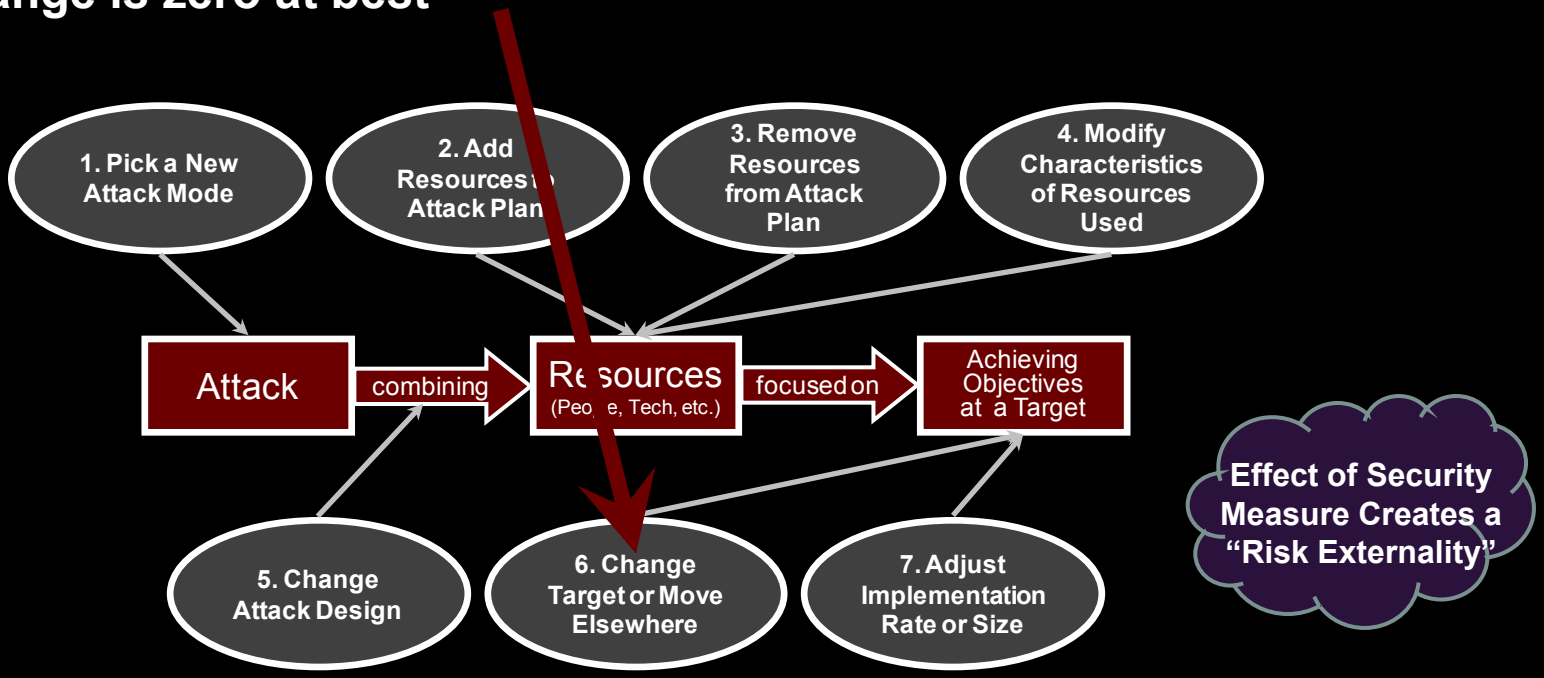
- **More complex attack design → Greater chance of attack failure when attempted → ΔRisk – at protected target**



Different Adaptation Paths Have Varied Effects On Risk… And Value Depends On Perspective

Attackers deciding to "take their business elsewhere" – change their target or operational area – may be a win, loss, or draw depending on perspective of analyst assessing it:

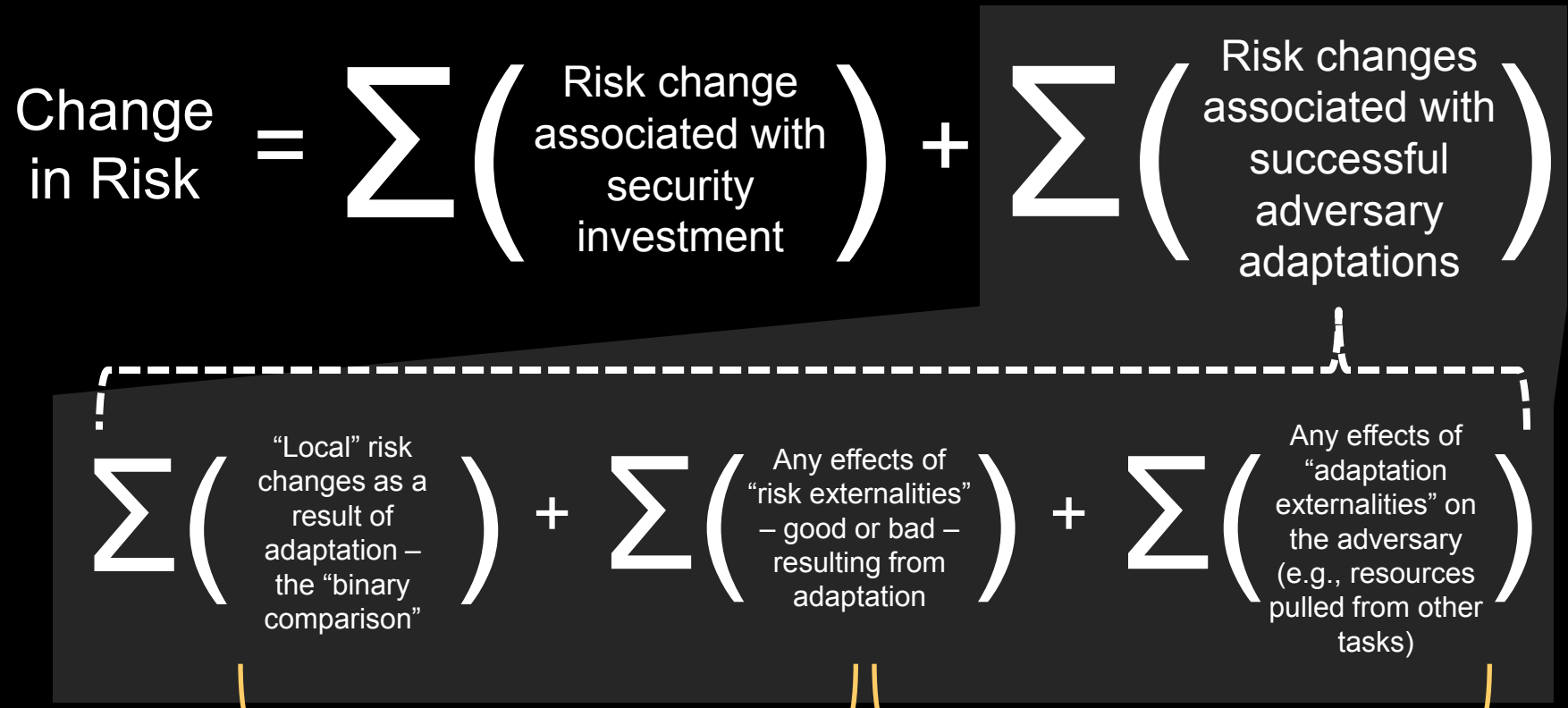
- **Effect is a ΔRisk – at the protected target, but…**
- **… if a comparable target is attacked elsewhere, then "globally" the change is zero at best**



…But "Adaptation Externalities" On The Adversary Side Also Shape Net Risk Effects Of Security

- Returning to the simple example where an attacker devoted 3x baseline resources to hide from a new detection measure…
- Where are those resources coming from?
  - Earlier slide assumed resources devoted to the target were constant
    - Therefore, attack rate dropped by 2/3
  - Does the group pull resources from elsewhere to make up for the loss?
    - If so, attack rate may not fall as much… and risk effect will depend on what activities are cut
  - Does the group try to raise new resources to make up the shortfall?
    - If so, the risks the group must accept to do so could be a key outcome

Risk Effect of Security Measures Given Adversary Adaptation Is Therefore a Sum Of Sums



Even Qualitative Analysis of Adaptation Stimulated By Different Security Measures Could Aid Planning

- For a specific measure:
  - Which adaptation pathways are relevant to the measure, and what types of risk effects will they produce?
- For a particular adversary of interest:
  - Are there detectable preferences for which adaptation paths are considered, and how different options are weighed?
- For a specific measure *plus* an adversary of interest:
  - Are the "net sums" of the effects from the measure, adaptation to the measure, the risk externalities, and the adaptation externalities on the adversary likely to be large or small?

Even approximate or qualitative answers to these types of questions could be applicable to some portfolio analyses or "adaptation sensitivity" analyses security options

Briefing Outline

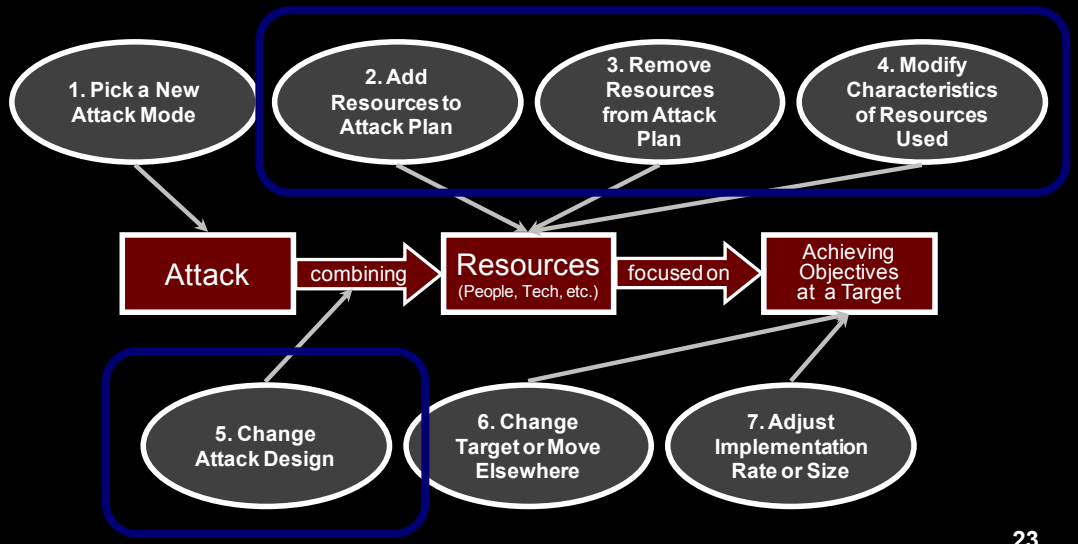
- **What we know about adversary adaptation to security measures**
  - **Characterizing the range of options available to adversaries**
  - **Understanding the factors that shape the choices that they make and their ability to change effectively**
- **Building a comprehensive picture of adaptation *effects* on risk**
  - **Analyzing the effect of different types of adaptation on security effectiveness**
  - **Understanding how "adaptation externalities" groups face affect the risk they pose more broadly**
- **Concluding observations on analysis and data collection needs**

Anticipating Adaptation Effect Requires Linking The First Part Of Briefing To The Second

- **Anticipating attacker behavior requires drawing on what we know about group behavior and psychology**
  - Is new detector viewed as a threat or an opportunity? Or neither?
  - If a threat, is the path chosen "offensive" or "defensive?"
- **Analysts also must be sensitive to the *realistic decision making environment* in adversary groups**
  - We cannot assume away their severe information challenges and idiosyncratic behaviors
  - It is highly unlikely that a group will have the information and capability needed to respond "optimally" to a defense
- **We also must figure out how to at least make estimates of the risk effects of the various types of externalities**
  - Easier → location or target risk displacement
  - Harder → effect on group's other activities, etc.

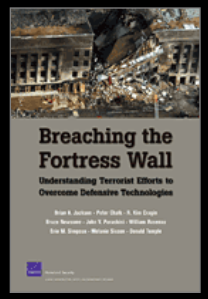
But… There are Significant Data Issues Associated With What Needs To Be Done

- **Foundational work on adversary adaptation to defensive measures has been done using open source data**
  - **Ex: Sandler *et al.* work on displacement among target types**
  - **RAND case studies of group adaptation behavior and learning**
- **A new weapon type or a targeting shift are very "visible" adaptations for observers outside an adversary group**
  - **But they are only part of the picture**
- **Other adaptation types (and changes not directly related to attack operations) are nearly invisible in the data sources used for most such analyses**



Important Data Needed To Anticipate Behavior Are Also Internal To Adversary Groups

- **Characterizing adversary decision making requires visibility (or at least some insight) into their internal deliberations and preferences**
  - This can be done in some cases through detailed cases studies where information is available in the open source
  - We are experimenting with doing this using public discourse from a group (jihadi internet discussions)
  - However, collected intelligence would be a more direct – and likely more representative – source



- **Assessing – or even sometimes *identifying* – some of the important externalities similarly depends on data internal to groups**
- **Analysis requires ways of either estimating these effects or marrying open with closed source data**

Homeland Security and Defense Center

A MULTI-UNIT RESEARCH CENTER